Montana Information Security Advisory Council

Meeting Minutes
September 16, 2015

Attendees	
Meeting Chairperson: Lynne Pizzini, State Information Security Officer	
Name	**Affiliation**
Erika Billiet	**Local Governments**
Joe Chapman	**Department of Justice**
Bryan Costigan	**MATIC/Department of Justice**
John Daugherty	**Department of Corrections**
Sherri Davidoff	**LMG Security**
Kreh Germaine	**Department of Natural Resources & Conservation**
Jim Gietzen	**Office of Public Instruction**
Adrian Irish	**Montana University System**
Margaret Kauska	**Department of Revenue**
Rep. Kelly McCarthy	**(D) HD 49**
Major General Quinn	**Director of Military Affairs, Montana National Guard**
Meeting Minutes recorded by: Samantha Cooley, SITSD	

Meeting Guests: Sky Foster, AG; Bill Genzoli, Xeorx/ATOS; Michael Barbere, SITSD; Lisa Vasa, SITSD; Eric Durkin, Northrup Grumman; John Burrell, MATIC/DOJ; Dawn Temple, JISTD/DOJ; Barry Wall, SITSD; Joe Frohlich, SITSD; Tom Manderville, DOR; Sean Rivera, SITSD

🖰**Real-Time Communication:** Kristin Burgoyne, George Parisot, Josh Rutledge, Joshua Tuman, Chris Kuntz, Matt Pugh, David Swenson, Sven Taffs

I. Welcome & Introductions, Lynne Pizzini

Governor Bullock will be at the October 21, 2015 MT-ISAC Meeting.

Approval of August Meeting Minutes: The August, 2015 MT-ISAC Meeting Minutes were approved as written.

II. Legal Opinion on State Policy, Mike Manion

At the last MT-ISAC Meeting, there was discussion on potential liability issues resulting from implementing the Five Core Security Policies. It was decided that the policies would be subject to a legal review by Mike Manion. Mike is reporting his findings today.

Findings:

1. When there are policies in place that we are not in compliance with, there is always potential a liability issue. The claim in the liability would be negligence. Negligence is a common law claim that occurs when organizations do not live up to a “reasonable standard of care” in the industry.

2. Under Montana law, there are statutes that require the State to adopt policies. Executive Branch Statute 2-15-114 MCA states "the department shall develop written policies to ensure the security of data." Under that statute, if a policy isn't adopted and an incident takes place, an agency could be found negligent by not adopting the written policy to ensure data security, and as a result of that, damage was caused.

3. Montana Information Technology Act 2-17-512, states the DOA, through SITSD, is statutorily required to adopt and enforce Statewide information technology policy and statute. It does not specify what policy.

4. Liability can't be avoided by failing to adopt policy. The reasonable entity standard will be applied in a negligent situation. If it is the industry standard, organizations can be held liable.

Recommendation: Regarding the implementation of the Five Enterprise Security Policies, it is better to have a policy in place, including exceptions to identify/explain areas out of compliance. Policies that are adopted should be reasonable, industry standards.

Justification for Recommendation: The standard practice with audits is that a written policy be in place. Auditors want to know if the policy is being followed, and if not, they want to know why. Insurance companies require policies to cover potential risk.

Proposal: Sherri Davidoff proposed adopting the Five Enterprise Security Policies along with corresponding Action Plans for each agency. In the private sector, LMG Security is required to create a suite of policies for customers that previously had no policies. Implementation Plan's and documented notes for auditors are included.

Mike Manion commented Sherri's suggestion would decrease liability. A judge or a jury can look at that and say, with good faith, full implementation is being pursued. From a practical perspective, it would be a good step.

Margaret Kauska commented the DOR's Corrective Action Plan Annual Report with the IRS includes a Plan of Action and Milestones, POAM. Making progress and understanding that obtaining perfection is ideal, yet unrealistic, is important.

FISMA/NIST at the Federal Level

John Daugherty commented that the Federal Government implemented something similar regarding FISMA and NIST. Agency heads have one year to develop and implement an action plan. In the action plan, full documentation of items applicable and not applicable to agencies is required. Agency heads report to the Office of Management and Budget annually on progress and status.

John suggested that Montana adopts a similar process. Montana already has a requirement statute for the Technology Plan including a "Security" section. Adoption of an Action Plan would provide a template for agencies, providing consistency and clarity on requirements.

Customizing Plans for Agencies

Kreh Germaine expressed the importance allowing customizable plans for agencies, as each agency has different types of data and data requirements. Agency heads should be provided the opportunity to tailor plans to meet the unique needs of their organization. Developing a recommended path forward for agencies and implementation plan timeframe will be important. The potential to being out of compliance, lacking time and resources to implement requirements, needs to be mitigated.

John Daugherty shared some information from the OMB.

Q1: Are NIST guidelines flexible?
A1: Yes, while agencies are required to follow the requirements in the policy, there is flexibility in how these requirements are applied.

Q2: Are agencies required to select and implement all security controls?
A2: No, agencies are required to use a risk based approach in implementing Security Plans. They should provide documentation in areas where they are not implementing certain controls.

Kreh Germaine recommended that we add similar language to the policy, to prevent liabilities and improve the State's security posture.

Lynne Pizzini commented there is similar language in the current Risk Management Policy. When the Baseline Security Controls were adopted, Montana adopted 176 out of the 230 controls. From a moderate control perspective, some of the controls did not apply to the State.

III. Five Enterprise Security Policy, Lynne Pizzini

These polices have been presented and discussed. It was recommended from the Enterprise Risk Assessment (audit) that took place last summer that the Enterprise Security Policies need to updated according to the new Cybersecurity Framework. The proposed policies are a new way to present existing policies, for agencies to use as templates.

Inquiry, Kreh Germaine:

"Based on what John (Daugherty) was commenting on, regarding flexibility, where is that in policy?"

Response, Lynne Pizzini:

"We can add a statement to these polices that will have an implementation timeline, whatever we agree is reasonable."

Inquiry, Bryan Cositgan:

"If we add an implementation timeline, we need to be thinking about metrics and how we can capture that measurement. How will we address that? Would we use a percentage of progress made and provide documentation?"

Response, Lynne Pizzini:

"This council will need to make a recommendation on that. One of the Workgroups can make a recommendation, developing a process for implementation and identifying a method to measure progress."

Kreh Germaine commented before voting to adopt the policies, he would like to see language included that addresses the following areas:

- Implementation Plan and Timelines
- Flexibility on what requirements agencies adopt
- Agency heads are provided flexibility and authority in creating their plans

Lynne commented that the current policy talks about application to agencies, it has already been addressed.

Implementing a Reasonable Timeline

Considerations:

- It will be difficult to develop a timeframe that meets all agency requirements. Agencies may better set up for success with the OMB Language.
- It's important for agencies to come up with their own plan, a maximum timeframe needs to be identified.
- Federal agencies have been trying to implement NIST for years, this a lengthy process.
- Require reporting on implementation progress after the set five year term.
- Currently, agencies are allowed to make exceptions. If there is a requirement they cannot obtain within the set time or feel it does not apply, they can be granted an exception request.
- A timeframe of one year is to short, five years is too long.
- MT-ISAC has the authority to change these policies and the deadlines identified within.
- There are limited agency resources (personnel and budget funds) available to assist with implementing these policies.
- The Enterprise Security Program is able to help agencies customize and deploy implementation plans. The program is a resource available to agencies and will work with agencies on their Yearly Progress Updates.

Sherri Davidoff proposed a motion to adopt the policies, further requiring an implementation plan that is executed by agencies within three years.

General Quinn responded that three years is concerning given it's only one legislative cycle away. If funding requests that are not successful, then a three year implementation timeline will not be met, requiring the submission of an exception, which can be problematic. General Quinn would prefer two legislative cycles, pushing it back to five years. While this is a long time, there are only two chances to get this through the session. General Quinn proposed changing the language in the motion to "adopt the proposed enterprise security policies, requiring an implementation plan from each agency, with the objective to have the plan implemented within three years, not to exceed five years."

Motion: Sherri Davidoff amended her previous motion and motioned to accept the Five Enterprise Security Policies with the requirement of an implementation plan. Agencies will work towards implementation in a three year period, not to exceed five years, with yearly implementation status updates from each agency. General Quinn seconded the motion. All were in favor. The motion carries.

Inquiry, Bryan Costigan:

> "Will SITSD create an overall implementation plan once the other plans are in?"

Response, Lynne Pizzini:

> "Yes, the Enterprise Security Program will take on that responsibility."

Thank you to Michael Barbere for all of his hard work on these policies.

IV. **Baseline Security Controls, Lynne Pizzini**

This document was accepted last year. All of the old security policies are now contained in the one document as the Baseline Security Controls. Today will be a review of the Baseline Controls and the information that has been added to them. At the October meeting, the old polices will be brought forward to be rescinded.

Inquiry, Kreh Germaine:

> "I was had the understanding that the 28 Security Policies were being exonerated into the Five Policies we just voted on?"

Response, Lynne Pizzini:

> "The Five Enterprise Security Policies that we just voted on are the Baseline Security Controls in a different format. The reason we developed the five policies is so agencies can use them as a template. They comply with NIST and the new Cybersecurity Framework outline. The Baseline Security Controls are designed to contain all the information in one document."

Response, Joe Frohlich:

> "The Baseline Security Controls are more specific to the State of Montana, the Five Enterprise Security Policies are more specific to NIST and the Cybersecurity Framework."

Inquiry, Kreh Germaine:

> "If we are meeting the five policies but we are getting stung on the Baseline Controls, are we still liable? I feel like we have two documents guiding us and there is going to be confusion."

Response, Lynne Pizzini:

> "The only document that we, as a State, will be looking at for compliance is the Baseline Security Controls. The Five Enterprise Security Policies are at a higher level, they don't get in as deep as the Baseline Controls. For example, a password has to have a minimum of eight characters, that is not spelled out in the Five Policies"

Inquiry, General Quinn:

> "If we are meeting the Five Policies, could we still be in violation of the Baseline Controls? Is it possible to meet one and not the other?"

Response, Lynne Pizzini:

“No if you meet one, you meet the other.”

Inquiry, Sherri Davidoff:

“Does one require the other?”

Response, Joe Frohlich:

“There is the document that ties the Framework to NIST.”

Response, Lynne Pizzini:

“The Baseline Security Controls follow NIST 800-53, the Five Policies are grouped into five different areas, which have 18 different families. The Baseline Security Controls are included in the Cybersecurity Framework, just in a different fashion. Pull up the document from the September meeting, it will show this relationship better. The feds look at this from both directions. That is why we decided to adopt policies that do the same.”

Inquiry, Bryan Costigan:

“Do you think we need an introduction or guidance document that sits in front of both of these, that explains what is overarching etc. to people because I can understand how it would be easy to get confused without instruction or guidance.”

John Daugherty commented his understanding was these were companion documents. The controls exist as an attachment to one of our policies, so you have taken the existing attachment (the Baseline Controls) and then taken all of the things that were in policy and really should have been in the control document and moved them in there. This isn’t anything new, simply conversion into one document. Joe Frohlich and Lynne Pizzini confirmed that is correct.

Inquiry, General Quinn:

“We just made a motion and agreed that everyone should adopt the Five Framework Policies, that may be easier to meet than the Baseline Controls. There may be State Policy out there, that I am unaware of, that states each agency must meet the Baseline Security Controls. Should the motion have been on the Baseline Security Controls opposed to the overarching policy if it isn’t tied directly to the Baseline Controls? If the overall policy/motion says agencies will meet each of the requirements tied into the Baseline Controls document up to the Five Enterprise Security Policies, what is required of agencies would be more clear, as opposed to what will met Fed requirements (Five Enterprise Security Policies) vs. what agencies will be graded on (Baseline Controls).”

Response, Michael Barbere:

“What we are looking at with the Baseline Security Controls is a specific control implementation guideline. The Framework is specific policy prescriptive guidelines. The overarching prescriptive guidelines will help meet the specific control objectives. So we have the policy prescriptive guidelines (Five Enterprise Security Policies) the baseline controls give specific prescriptive guidelines on how to meet that objective.”

Inquiry, Jim Gietzen:

> *"*Are they requirements or guidelines?"

Response, Mike Barbere:

> "That is flexible, there are security categorizations, we have flexibility built into that. There is low, moderate or high security categorizations that are built into policy. You can adjust up or down. The categorization is flexible in that respect. You don't have to implement every single control. It depends on the classification on the information system. In the policies we just adopted, they state agency heads are responsible for assigning security classifications to their information systems. Any risk must be well documented and signed off on ."

Jim Gietzen recommended mapping the Baseline Controls into the Five Enterprise Security Policies so there is only one document, it will create less confusion. Agencies are held to the strictest policy out there, the Five Policies aren't needed if we have the Baseline Controls.

Lynne Pizzini commented this is an effort to consolidate the 29 policies into one, so people don't have to look into multiple places to find all of the security policies. These need to be in place because of the Federal requirements to do so. Michael Barbere commented this is an expression of due diligence, there is a level of liability associated with not adopting the Baseline Controls or the Five Enterprise Policies.

Inquiry, Erika Billiet:

> "Would it be safe to say the Five Enterprise Security Policies are a starting point in the process?"

Response, Lynne Pizzini:

> "I am considering mapping the Baseline Controls back to the Five Enterprise Security Policies."

Jim Gietzen commented this would make it much easier for agencies.

Action: SITSD will map each of the Baseline Controls back to the Five Enterprise Security Policies.

Motion: Sherri Davidoff motioned to combine all of the Security Policies into one document with the Baseline Security Controls. John Daugherty seconded the motion. All were in favor. The motion carries.

The Baseline Security Controls will be an appendix to the Five Enterprise Security Policies. It will become part of the policy, which will help clarify requirements for agencies.

Action: The Enterprise Security Program will provide an update at the October meeting on their progress in mapping the Baseline Controls to the Five Enterprise Security Policies.

V. <u>DOR Joint Task Force – Fraud & Identify Theft Update, Lynne Pizzini</u>

On September 1, 2015 the Department of Revenue's Director, Mike Kadas, held a meeting on fraud and identify theft for the State. At that meeting agencies shared their experiences with fraud and identity theft. The DOR has a great amount of experience with attempts of identity theft, as do several other agencies. As the conversation carried on, the topic moved to securing data. The lack there of, leads to identity theft and fraud. Continuation of the discussion indicated that education on data protection and communication are key to prevention. Other topics of discussion included:

- Potential future legislation that includes fees for breaches of security that lead to fraud/identity theft
- Sharing best practices
- Software and vendors that can assist in alleviating the problem
- Funding was identified as need
- A Cyber Response Unit was recommended through the DOJ
- Coordinating efforts with MT-ISAC, Lynne Pizzini, Margaret Kauska are members of the Task Force

Action: Anyone interested in participating on the DOR Joint Task Force, please contact Lynne Pizzini, Margaret Kauska or Lee Baerlocher.

John Daugherty will be attending the meetings going forward.

VI. Workgroup Reports

Goals & Objectives Workgroup, Joe Chapman

This group consists of Joe Chapman, Margaret Kauska, Adrian Irish, Kreh Germaine and Joe Frohlich. They met a few times and went over the Strategic Goals and Objectives, the group thought it made sense to reorganize it under the NIST Framework. The changes made are as follows:

1. Purpose: states the Governor’s Executive Order.
2. Guiding Principles: there were some objectives that were more “guiding objectives”. This list was added directly under “Purpose”.
3. Mission: the first objective on the previous document was changed to the Mission.
   “The mission of the State of Montana’s Information Security Advisory Council (MT-ISAC) is to recommend an integrated interagency information security strategy to enhance the State information security posture.”
4. The Goals and Objectives were placed in an outline using the NIST Framework.
5. Sub-objectives were added.

The group has yet to receive any comments/changes on the new version. Lynne thanked the group for taking the time to put this together.

General Quinn commented there may be States other than Washington that Montana decides to model and proposed striking “Washington” from 2.3.1:

> *“Evaluate ~~Washington~~ other States best practices and training of the cyber unit of the National Guard and apply similar practices in Montana where applicable (DOA, DOJ, National Guard etc.)”*

Motion: The Goals and Objectives Workgroup motioned to accept the revised Goals and Objectives with the correction (as stated above). All were in favor. The motion carries.

Situational Awareness Workgroup, Bryan Costigan
The group has met one time; there was good participation in the meeting. A summary of the meeting is as follows:

- Roles in Situational Awareness: consumers, customers, contributors.
- The group is identifying what information they need to provide.
- Information needs request was sent out by John Burrell, MATIC.
- Timeliness of information is important.
- If information cannot be obtained and conveyed in a timely manner it provides no benefit.
- Political realities have been identified as a significant item for the group to address.
- The group is considering modifying reporting to SITSD, how it works and potential changes will be further defined.
- In the future, the group will work on sharing information with private sector partners.
- John Burrell is working on anonymizing information they receive for reporting purposes.

A special thank you goes to Dawn Temple for taking notes at the meeting.

VII. Formation of Suggested Workgroups

Joe Frohlich and Lynne Pizzini had a discussion on workgroups today and considered basing the Workgroups form the Goals and Objectives that were adopted today. Lynne suggested five different workgroups to address the five different areas of goals and objectives. Lynne asked the group to comment and provide further recommendations.

Considerations:

- Legislative would fall under "Governance" or "Identify".
- Sherri Davidoff commented we need a Workgroup that focuses on micro-organizations (small agencies, local governments) and what their needs are. Lynne commented we would develop this group further down the line after one year to 18 months.
- Concern that basing the Workgroups from the Goals and Objectives will become too foggy and vague. The specific Workgroups previously identified will be more beneficial.
- Workgroups should be correlated with objectives so the group stays on task.
- Defining what the Workgroups are may be a good opportunity for electronic polling to see who is interested in doing what.
- Some of the Workgroups should take precedence. A plan on identifying how this will move forward is important in keeping the group from being spread too thin.
- Reaching out to members outside of the MT-ISAC is recommended and found to be beneficial.

Proposed Workgroup Descriptions:

Security Team Development: work with the Enterprise Security Program and implementation of the Baseline Security Controls.

Legislative Workgroup: works on issues related to legislation.

Governor Dashboard: report to the Governor on statistics related to cybersecurity.

Public Safety: educating the public on issues related to cybersecurity.

Cyber Environment: this addresses the cyber environment in the State of Montana, analyzes cyber education and cyber businesses and bringing them together.

Outcomes:

- Joe Frohlich will work on a survey to define the MT-ISAC Workgroups. There will be three to five Workgroups established.

Action: Committee members should send recommendations for suggested Workgroups to Joe Frohlich. Joe Frohlich will put together a survey to be sent to the committee and will report back at the October meeting.

VIII. Current Threats, Sean Rivera

Vulnerabilities:

1. Bluetooth Vulnerability in iPhone and MAC devices that uses AirDrop. This can affect devices that are not jailbroken. The only way to fix this is to upgrade to IOS Version 9.
2. Cisco Router: SYNful Knock. This is a malware that is being observed on CISCO routers. Has been observed on 14 different routers worldwide. Network administrators credentials can get owned by the attacker. This only works on HTTP. They cannot access malware using SSH or HTTPS.

IX. Cybersecurity Training, Lisa Vasa

Information Security Training and Awareness October, 2015

This year's theme is "Stay Safe on the Information Highway."

Formal Awareness Training

- Mandated by Governor Bullock for all executive branch agencies
- Encouraged for other State organizations
- Annual training required
- SANS Securing the Human
    - Diverse Training needs
    - Complete set of training modules
    - Provided to State organizations at no additional costs
    - Licenses available for purchase by other organizations
    - Net training year starts on October 1
- SANS STH Phishing, there is a limited number of licenses. Over the next year we there will be some limited phishing exercises with staff.

Ongoing Awareness Activities

- Monthly Security Newsletter and materials
- Different security topics each month
- Posters, security tips, handouts, news

- Information about security awareness events all year long. Lisa will be reaching out to MT-ISAC Members to host events at their locations.
- Montana IT Conference

Information Security Events

- Monthly beginning in October 2015
- Three interactive activities with handouts, giveaways and treats
- Examples of handouts and October posters are available on the table at the end of the meeting
- Gift cards, Auto emergency kit, 2 Microsoft Surfaces will be given away this year

October Event Schedule

October 8 – SMDC Helena 2:00 – 4:00 pm
October 14 – Mitchell Bldg. Rm 52 10:30 am – 2:00 pm
October 21 – Capitol Rotunda 11:00 am – 4:00 pm *next MT-ISAC Meeting. Please stop by before or after the meeting.
October 22 – Cogswell Bldg. 11:00 am – 2:00 pm
October 27 – Mitchell Bldg. Rm. Five3 10:30 am – 2:00 pm

Montana IT Conference – December 7-11, 2015
Tracks include:

- Starting with Security
- Introduction to System Security Plans and Risk Assessments
- Creating Effective Security Training & Awareness Programs
- Digital Forensics (panel discussion)
- Physical Security
- Two additional sessions *to be announced*
- Four hour Disaster Recovery Tabletop Exercise, Department of Homeland Security

CPE's: up to 10 CPE's available. The full conference agenda will be available on October 1.

Professional Training

- SANS Professional Training
- Federal Virtual Training Environment, free to Governmental agencies
- Other training providers for limited or no cost are being researched
- Updates will be in the Security Newsletter

Graphics will be part of the packets provided to agencies. Agencies are encouraged to use these graphics in their newsletters, communications etc. Some of the materials are customizable and have a Zazzle store available to print materials. Lisa will ensure agencies have digital copies of all of the information. There are links to the resources on the website.

The Montana IT Conference is open for private sector members to attend.

SITSD will be asking everyone to take the SANS Security Training again. It is mandated this training needs to completed on an annual basis. A Workgroup out of this council will be looking into the effectiveness of SANS Training. SANS updates their training once a year, their last update was fairly limited. This year, SANS updated more than usual. They created an Advisory

Panel to look at the scripts and conducted a poll to improve trainings. As a result of the poll, more interactive content will be included in the future.

Virtual Events: Margaret Kauska commented DOR is launching Cybersecurity Awareness on October 21. Including the field staff is very important, remote exercises (virtual events) are very useful.

Action: Joe Frohlich and Lisa Vasa will work on putting together a virtual event this year, designed for participation/completion online.

For more information on training, contact Lisa Vasa or Joe Frohlich.

Action: The November 3, 2015 Cybersecurity Training Event at the HHS Auditorium has not been finalized yet. Once it becomes finalized, Lynne Pizzini will send out information.

X. Open Forum

Cybersecurity Teams: General Quinn will schedule the National Guard Cybersecurity Team discussion after he goes to Washington, he will let Lynne know when this item should be added to the MT-ISAC Agenda.

XI. Public Comment

Bill Genzoli, Xerox offered to make their meeting place at the ____ (get from Joe) available for Cybersecurity Events.

Next Meeting Information:
Date: October 21, 2015
Time: 1:00 pm – 3:00 pm
Location: State Capitol, room 152

XII. Summary of Motions Passed

Motion: Sherri Davidoff amended her previous motion and motioned to accept the Five Enterprise Security Policies with the requirement of an implementation plan. Agencies will work towards implementation in a three year period, not to exceed five years, with yearly implementation status updates from each agency. General Quinn seconded the motion. All were in favor. The motion carries.

Motion: Sherri Davidoff motioned to combine all of the Security Policies into one document with the Baseline Security Controls. John Daugherty seconded the motion. All were in favor. The motion carries.

Motion: The Goals and Objectives Workgroup motioned to accept the revised Goals and Objectives with the correction (as stated above). All were in favor. The motion carries.

**Summary of action items begins on page 13*

XIII. Summary of Action Items

Action: SITSD will map each of the Baseline Controls back to the Five Enterprise Security Policies.

Action: The Enterprise Security Program will provide an update at the October meeting on their progress in mapping the Baseline Controls to the Five Enterprise Security Policies.

Action: Anyone interested in participating on the DOR Joint Task Force, please contact Lynne Pizzini, Margaret Kauska or Lee Baerlocher.

Action: Committee members should send recommendations for suggested Workgroups to Joe Frohlich. Joe Frohlich will put together a survey to be sent to the committee and will report back at the October meeting.

Action: Joe Frohlich and Lisa Vasa will work on putting together a virtual event this year, designed for participation/completion online.

Action: The November 3, 2015 Cybersecurity Training Event at the HHS Auditorium has not been finalized yet. Once it becomes finalized, Lynne Pizzini will send out information.

Meeting Minutes Draft Submitted by: Samantha Cooley
Date of Submission: September 28, 2105